AMENDMENTS TO THE CLAIMS

The listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims

1. (Currently Amended) A method for password-based authentication in a communication system ~~comprising~~ including a group ~~(100)~~ of at least two units ~~(12; 22; 32; 42; 52; 72; 82; 92)~~ associated with a common password, ~~characterized by~~ comprising the steps of

assigning individual authentication tokens to the respective units in the group based on the password such that each authentication token is irreversibly determined by the password;

determining, at a first unit ~~(32-1; 42-1; 52-2; 92-1)~~, a check token for a second unit ~~(32-2; 42-2; 52-1,52-3, 52-4; 92-4)~~ based on the password and the authentication token of the first unit; and

comparing, at the second unit, the check token with the authentication token of the second unit for authentication of the first unit towards the second unit.

2. (Currently Amended) The method of claim 1, ~~characterized by the~~ further comprising the step of

deleting the password and all significant parameters generated in the authentication procedure except the authentication tokens after usage thereof.

3. (Currently Amended) The method of claim 1, ~~characterized by the~~ further comprising the step of

accepting, at the second ~~unit~~ unit, ~~(42-2; 52-1,52-3, 52-4; 92-4)~~ ~~and~~ in response to a successful authentication, update information securely transferred from the first unit ~~(42-1; 52-2; 92-1)~~, at least a portion of the update information being created at the first unit.

4. (Currently Amended) The method of claim 3, ~~characterized in that~~ wherein the update information is associated with revocation of a non-trusted group member.

5. (Currently Amended) The method of claim 3, ~~characterized in that~~ wherein the update information relates to a password change.

6. (Currently Amended) The method of claim 3, ~~characterized in that~~ wherein the update information is selected from the group of :

new authentication tokens,

a new group key, a group-defining list, and

a revocation list ~~(45; 55; 95)~~, including combinations thereof.

7. (Currently Amended) The method of claim 3, ~~characterized by delegation of~~ further comprising the step of delegating update rights to a third intermediate unit ~~(92-2,92-3)~~, and sending at least a portion of the update information for the second unit ~~(92-4)~~ to the intermediate unit.

8. (Currently Amended) The method of claim 7, ~~characterized in that~~ wherein the update information is accompanied by a time stamp for determining whether the update information is still valid when the intermediate unit ~~(92-2,92-3)~~ encounters the second unit ~~(92-4)~~.

9. (Currently Amended) The method of claim 7, ~~characterized in that~~ wherein the delegation of update rights comprises delegation of rights to further delegate update rights.

10. (Currently Amended) The method of claim 1, ~~characterized in that~~ wherein the assigning step ~~in turn~~ further comprises the steps of

determining, at an assigning unit ~~(72-1; 82-2)~~ in the group, a token secret common for the group and non-correlated with the password; and

creating, at the assigning unit, the authentication token for another unit ~~(72-2,72-3 ; 82-4)~~ in the group based on the token secret and the password.

11. (Currently Amended) The method of claim 10, ~~characterized in that~~ wherein the step of determining the token secret involves generating the token secret, as a part of an initial set-up procedure.

12. (Currently Amended) The method of claim 1, ~~characterized in that~~ wherein the step of determining the check token ~~in turn~~ further comprises the steps of

retrieving, at the first unit ~~(32-1; 42-1; 52-2; 92-1)~~, the token secret using the authentication token of the first unit and the password; and

creating, at the first unit, the check token for the second unit ~~(32-2; 42-2; 52-1,52-3, 52-4; 92-4)~~ based on the token secret and the password.

13. (Currently Amended) The method of claim 10 ~~or 12~~, ~~characterized in that~~ wherein the creating step involves using a bijective locking function, the input parameters of which include the token secret and a one-way function of the password.

14. (Currently Amended) The method of claim 13, ~~characterized in that~~ wherein the locking function is a symmetric encryption function.

15. (Currently Amended) The method of claim 13, ~~characterized in that~~ wherein the locking function is implemented through password-based secret sharing.

16. (Currently Amended) The method of claim 1, ~~characterized by~~ wherein implementing policies in at least one of the units in the group for limiting the number and/or frequency of authentication attempts.

17. (Currently Amended) The method of claim 1, ~~characterized by the~~ further comprising the step of generating an alarm signal if the number of authentication attempts exceeds a predetermined value.

18. (Currently Amended) The method of claim 1, ~~characterized by the~~ further comprising the step of sending an authentication response message ~~(34; 44; 94)~~ from the second unit ~~(32-2; 42-2; 92-4)~~ indicating the result of the comparing step.

19. (Currently Amended) The method of claim 1, ~~characterized by~~ further comprising the step of authentication of the second unit ~~(32-2; 42-2; 52-1,52-3, 52-4; 92-4)~~ towards the first unit ~~(32-1; 42-1; 52-2; 92-1)~~, whereby the first and second units are mutually authenticated towards each other.

20. (Currently Amended) The method of claim 19, ~~characterized by~~ further comprising the steps of:

generating a respective random value at the first and second unit;

determining temporary test secrets at the first and second unit based on the random values; and

exchanging the temporary test secrets between the first and second unit for mutual authentication purposes.

21. (Currently Amended) The method of claim 1, ~~characterized in that~~ wherein critical operations for which authentication is needed are listed in policies in at least one of the units ~~(12; 22; 32 ; 42; 52; 72; 82; 92)~~.

22. (Currently Amended) The method of claim 3, ~~characterized in that~~ wherein a unit ~~(42-2; 52-1,52-3, 52-4; 92-4)~~ that is switched-on after being inactive for a predetermined period of time automatically requests appropriate update information from at least two other units.

23. (Currently Amended) The method of claim 1, ~~characterized in that~~ wherein the group ~~(100)~~ of units constitutes a Personal Area Network (PAN).

24. (Currently Amended) The method of claim 1, ~~characterized in that~~ wherein the authentication tokens are tamper-resistantly stored in the respective units ~~(12; 22; 32; 42; 52; 72; 82; 92)~~.

25. (Currently Amended) A communication system including a group ~~(100)~~ of at least two units ~~(12; 22; 32; 42; 52; 72; 82; 92)~~ associated with a common password, and means for password-based authentication, ~~characterized by~~ comprising:

means for assigning individual authentication tokens to the respective units in the group based on the password such that each authentication token is irreversibly determined by the password;

means for determining, at a first unit ~~(32-1; 42-1; 52-2; 92-1)~~, a check token for a second unit ~~(32-2; 42-2; 52-1,52-3, 52-4; 92-4)~~ based on the password and the authentication token of the first unit; and

means for comparing, at the second unit, the check token with the authentication token of the second unit for authentication of the first unit towards the second unit.

26. (Currently Amended) The system of claim 25, ~~characterized by~~ further comprising

means for deleting the password and parameters generated in the authentication procedure except the authentication tokens after usage thereof.

27. (Currently Amended) The system of claim 25, ~~characterized by~~ further comprising

means for transferring update information from the first unit ~~(42-1; 52-2; 92-1)~~ to the second unit ~~(42-2; 52-1,52-3, 52-4; 92-4)~~; and

means for accepting, at the second unit, update information from the first unit in response to a successful authentication.

28. (Currently Amended) The system of claim 27, ~~characterized in that~~ wherein the update information is associated with revocation of a non-trusted group member.

29. (Currently Amended) The system of claim 27, ~~characterized in that~~ wherein the update information relates to a password change.

30. (Currently Amended) The system of claim 27, ~~characterized in that~~ wherein the update information is selected from the group of : new authentication tokens, a new group key, a group-defining list, and a revocation list ~~(45; 55; 95)~~, including combinations thereof.

31. (Currently Amended) The system of claim 27, ~~characterized by~~ further comprising means for delegation of update rights to a third intermediate unit ~~(92-2,92-3)~~, and means for sending at least a portion of the update information for the second unit ~~(92-4)~~ to the intermediate unit.

32. (Currently Amended) The system of claim 25, ~~characterized in that~~ wherein the means for assigning ~~in turn~~ further comprises

means for determining, at an assigning unit ~~(72-1; 82-2)~~ in the group, a token secret common for the group and non-correlated with the password; and

means for creating, at the assigning unit, the authentication token for another unit ~~(72-2,72-3 ; 82-4)~~ in the group based on the token secret and the password.

33. (Currently Amended) The system of claim 25, ~~characterized in that~~ wherein the means for determining the check token ~~in turn~~ further comprises

means for retrieving, at the first unit ~~(32-1; 42-1; 52-2; 92-1)~~, the token secret using the authentication token of the first unit and the password; and

means for creating, at the first unit, the check token for the second unit ~~(32-2; 42-2; 52-1,52-3, 52-4; 92-4)~~ based on the token secret and the password.

34. (Currently Amended) The system of claim 32 ~~or 33~~, ~~characterized in that~~ wherein the means for creating involves a bijective locking function, the input parameters of which include the token secret and a one-way function of the password.

35. (Currently Amended) The system of claim 25, ~~characterized by~~ wherein policies implemented in at least one of the units in the group for limiting the number and/or frequency of authentication attempts.

36. (Currently Amended) The system of claim 25, ~~characterized by~~ further comprising means for generating an alarm signal if the number of authentication attempts exceeds a predetermined value.

37. (Currently Amended) The system of claim 25, ~~characterized by~~ further comprising means for sending an authentication response message ~~(34; 44; 94)~~ from the second unit ~~(34-2; 42-2; 92-4)~~.

38. (Currently Amended) The system of claim 25, ~~characterized by~~ further comprising means for mutual authentication between two units ~~(12; 22; 32; 42; 52; 72; 82; 92)~~ in the group.

39. (Currently Amended) The system of claim 25, ~~characterized by~~ wherein policies defining critical operations for which authentication is needed.

40. (Currently Amended) The system of claim 25, ~~characterized by~~ wherein said communication system being a Personal Area Network (PAN).

41. (Currently Amended) A first device ~~(12; 22; 32; 42; 52; 72; 82; 92)~~ belonging to a group ~~(100)~~ of at least two devices associated with a common password, and ~~comprising~~ including means for password-based authentication, ~~characterized in that this~~ the first device comprises:

means for receiving a password; means for assigning individual authentication tokens to other devices ~~(72-2,72-3 ; 82-4)~~ in the group based on the password such that each authentication token is irreversibly determined by the password;

means for determining a check token for a second device ~~(32-2; 42-2; 52-1,52-3, 52-4; 92-4)~~ in the group based on the password and the authentication token of the first device ~~(32-1; 42-1; 52-2; 92-1)~~; and

means for transmitting the check token to the second device for authentication towards the second device.

42. (Currently Amended) The device of claim 41, ~~characterized by~~ further comprising means for deleting the password and parameters generated in the authentication procedure except the authentication token after usage thereof.

43. (Currently Amended) The device of claim 41, ~~characterized by~~ further comprising

means for creating update information for the second device ~~(42-2; 52-1, 52-3,52-4 ; 92-4)~~; and

means for securely transferring update information to the second device.

44. (Currently Amended) The device of claim 43, ~~characterized by~~ further comprising means for delegation of update rights to an intermediate device ~~(92-2,92-3)~~, and means for sending update information for the second device ~~(92-4)~~ to the intermediate device.

45. (Currently Amended) The device of claim 41, ~~characterized in that~~ wherein the means for assigning ~~in turn~~ further comprises

means for determining a token secret common for the group ~~(100)~~ and non-correlated with the password; and

means for creating the authentication token for another device ~~(72-2,72-3; 82-4)~~ in the group based on the token secret and the password.

46. (Currently Amended) The device of claim 41, ~~characterized in that~~ wherein the means for determining the check token ~~in turn~~ further comprises

means for retrieving the token secret using the authentication token of the first device ~~(32-1; 42-1; 52-2; 92-1)~~ and the password; and

means for creating the check token for the second device ~~(32-2; 42-2; 52-1,52-3, 52-4; 92-4)~~ based on the token secret and the password.

47. (Currently Amended) A computer program product for, when executed by a computer, password-based authentication in a communication system ~~comprising~~ comprising:

a group ~~(100)~~ of at least two units ~~(12; 22; 32; 42; 52; 72; 82; 92)~~ associated with a common ~~password, characterized by~~ password;

program means for assigning individual authentication tokens to the respective units of the group based on the password such that each authentication token is irreversibly determined by the password;

program means for determining, at a first unit ~~(32-1; 42-1; 52-2; 92-1)~~, a check token for a second unit ~~(32-2; 42-2; 52-1,52-3, 52-4; 92-4)~~ based on the password and the authentication token of the first unit; and

program means for comparing, at the second unit, the check token with the authentication token of the second unit for authentication of the first unit towards the second unit.